

SOC Incident Management System

IMS User Contact:	(b) (6),	Restrict Access To:	All IMS
Record Permissions Group:	All IMS Users	Record Source:	

Contact Details

Enter the NASA AUID or email address of the Contact, and click "Lookup Contact Details" to automatically retrieve the information.

AUID:	Email:
-------	--------

Enter Contact information below if the primary contact is not an IMS user

Contact Last Name:	(b) (6), (b) (7)(C)	Contact First Name:	(b) (6)
Contact Role:	NASA Other	Contact Office Phone:	
Contact E-mail:	(b) (6), (b) (7)(C)	Contact Cell Phone:	
Contact AUID:		Contact NASA Center:	
Contact Building:		Contact Room Number:	
Contact Type:			

General Details

SOC Tracking Number:	SOC-20160129-649963	Categorization:	Incident
Date Record Created (UTC):	1/29/2016 4:32 PM	Incident Time Zone:	UTC - Coordinated Universal Time Zone (GMT)
Title:	GSFC / GRC / AFRC: Possible Media Contact Regarding a NASA Data Breach		

SENSITIVE BUT UNCLASSIFIED

Brief Description:	<p>Email is attached. **email contains an attachment not opened by T1** SOC Recieved a message claiming to be from VICE News:</p> <p>I'm a journalist at VICE Motherboard. I have something important to ask you.</p> <p>A group of hackers has provided me with a large dataset that they claim they exfiltrated from NASA networks, in particular, those of the Glenn Research Center, the Goddard Space Flight Center and the Dryden Flight Research Center.</p> <p>The hackers say they had access to these networks for months last year, and have downloaded more than 250GB of data, including video and data logs from UAV flights. The hackers have provided me with a copy of the data, and plan to publish it online shortly.</p> <p>The data at first glance appears to be legitimate, but I wonder if you can confirm to be that there was a breach. I'm attaching a sample drone flight data log for you to review.</p> <p>Please let me know if you have any information about this alleged data breach,</p>		
Current Status:	Closed	Assigned To:	AFRC IRM AFRC IRT AFRC ITSM ARC IRM ARC IRT ARC ITSM (b) (6) GRC IRM GRC IRT GRC ITSM GSFC IRM GSFC IRT GSFC ITSM
Current Priority:	Low	Also Notify:	SOC Tier-3 SOC TVA
CUI:	No SBU or PII	Notify on Save:	No

US CERT Reporting

Risk Rating:		Functional Impact:	
Information Impact:		Attack Vectors:	Web
Recoverability:		Classified Incident:	
Critical Service or System:			

SENSITIVE BUT UNCLASSIFIED

Major Incident:

High Value Assets (HVA):

Reportable to Congress:

Observed Activity:

Number of Records Impacted:

Location of Observed Activity:

Number of Systems Impacted:

Actor Characterization:

Number of Users Impacted:

Action Taken to Recover:

Number of Files Impacted:

The fields below hold the US-CERT Reporting fields that were in force from October 1, 2015 through March 31, 2017. The are included here for reporting purposes only.

Functional Impact old: None

Informational Impacts old: None

Recoverability Impact old: Unknown

Related Tasks

Task ID	Assigned To	Due Date (UTC)	Priority	Status	Description	Resolution
650186	(b) (2), (b) (7) (E)	2/5/2016 9:57 PM	High	Complete	(b) (2), (b) (7)(E) (b) (6), (b) (7) (C) potential c2 domains for this incident	
650196	JSC IRM JSC IRT JSC ITSM (b) (6)	2/3/2016 12:00 AM	High	Complete	In the Data Dump from the parent ticket, the following statement is made: 1. (b) (6) 2. (b) (6) Axis IP Certified	(b) (6) (b) (6) n February 2, 2016 ~10:30AM CST, (b) (6) employed by (b) (6) and

3. Nasa (b) (7)(E)
Multimedia and Security Systems as a SMS Technician and is part of the Center Operations Directorate (JA). He works on cable installations.
4. Johnson Space Center

(b) (6) His contact information:
Mobile number: (b) (6)
" (b) (6) . He does not have a desk phone. (b) (6)

One of our associates (b) (6)
completely pwned this camera and appears to be his
network by ratting Randy Ross primary and only email
but we'll save that story address. His current
domain group memberships
for a rainy day" (b) (6)

(b) (6) act JSC user
(b) (6) and
investigate his system His current location is
for evidence of malware, in (b) (6)
specifically in the form (b) (6) His workstation is
of a Remote Access named
Trojan. (b) (6)
gov" and his current IP
address is:

SENSITIVE BUT UNCLASSIFIED

650300	SOC Tier-1	2/7/2016 7:38 AM	Medium	Complete	<p>*Please reassign to T1 when finished - please do not mark task as complete*</p> <p>US-CERT information request:</p> <p>NASA SOC,</p> <p>Is there an update available on this RFI? The Infowars.com article now includes the following "NASA Update":</p> <p>"UPDATE - NASA's Response to Hack Report:</p> <p>"Control of our Global Hawk aircraft was not compromised. NASA has no evidence to indicate the alleged hacked data are anything other than already publicly available data. NASA takes cybersecurity very seriously and will continue to fully investigate all of these allegations."</p> <p>Is this a legitimate update from NASA? We greatly appreciate your assistance.</p>	T2 did not release this statement to Infowars.com, but it was probably referencing a public statement made by HQ.
675238	(b) (2), (b)	8/12/2016 9:59 PM	Medium	Complete	<p>(b) (2), (b) (7)(E)</p> <p>(b) (2), (b) (7)(E)</p> <p>(b) (2), (b) (7)(E)</p>	

Related Incidents

Select Relationship: Related - SWI-20160201-650198

Relationship Description:

Parent Incident

SOC Tracking Number	Current Status	Title
---------------------	----------------	-------

No Records Found

SENSITIVE BUT UNCLASSIFIED

Child Incidents

SOC Tracking Number	Current Status	Title
---------------------	----------------	-------

No Records Found

Sibling Incidents

SOC Tracking Number	Current Status	Title
---------------------	----------------	-------

No Records Found

Incident Details

Time Incident Started:		Time Incident Started (UTC):	
Time Incident Detected:		Time Incident Detected (UTC):	
Center Affected by Incident:	Other	Overall Impact (reference):	Low
US-CERT Category:	CAT 6 - Investigations	Incident Subcategory:	
US-CERT Tracking Number:	INC000010050196	ESD Ticket #:	
Resolution Status:	Other	Malware Family:	
		Highest level of access gained:	
Primary Method used to Identify Incident:	Other - journalist		
Primary Attack Category:			
Primary Vulnerability Type:		Lost or Stolen NASA Equipment:	

Lost or Stolen NASA Equipment Application

Tracking ID	Cause of Loss	Type of System Lost	Description of Circumstances
-------------	---------------	---------------------	------------------------------

No Records Found

Host Information

NASA Hosts

IP Address	IPv6 Address	Host Name	Center/Facility
------------	--------------	-----------	-----------------

(b) (2), (b) (7)(E)

(b) (2), (b) (7)(E)

GSFC

External Hosts

SENSITIVE BUT UNCLASSIFIED

IP Address	External IPv6 Address	Host Name	Position in this attack
No Records Found			

Campaigns

Campaign Name:		Reviewed By TVA:	
Campaign Comment:		Confirmed By TVA:	
		Is APT:	

Indicators of Compromise

IOC Domain		
------------	--	--

FQDN	Do Sinkhole	Comment
No Records Found		

IOC IP

IP Address	IP Block	Comment
No Records Found		

IOC File

Filename	MD5 Hash	Comment
No Records Found		

IOC Registry Key

Key Name	Key Value	Comment
No Records Found		

IOC Email

Sender Email	Subject	Comment
No Records Found		

IOC Detection

Name	Type	Comment
No Records Found		

Root Cause Statement

The Root Cause Statement can be constructed from the following fields like so:

(b) (7)(E) ."

See the help for the individual fields for more information about what the various values mean and their context.

Root Cause Sources:

Root Cause Categories:

SENSITIVE BUT UNCLASSIFIED

Root Cause
Methods:

Root Cause
Factors:

Root Cause
Causes:

Root Cause
Objectives:

Reporting Organizations

Reporting Date (UTC)	Reporting Local Date	Reporting Local Time Zone	Reporting Notes	Reporting Number	Reporting Organization	Reporting Organization Contact
-------------------------	-------------------------	------------------------------	-----------------	------------------	---------------------------	--------------------------------------

No Records Found

Impact of Incident

NASA Programs,
Projects, and/or
Operations:

Data (at Rest or
Transmission):

Cost:

Number of
systems
affected by this
incident:

Number of
accounts
affected by this
incident:

Other Impacts:

Overall Impact: Low -- Incident Considered Low if none of the below Categories are rated Moderate or High

People:

System:

Sophistication /
Nature of
Attack:

Number of
NASA Centers/
Facilities
affected by this
incident:

Critical
Infrastructure
Impacted:

Containment Actions

Incident
Containment
System Action:

Incident
Containment
Network Action:

Recovery Actions

Incident
Recovery
System Action:

SENSITIVE BUT UNCLASSIFIED

Incident
Recovery User
Action:

Recommendations

Root Cause:

Lessons
Learned:

Costs

Center (Hours): 289.00

Center (Dollars): 28900.00

NASA SOC
(Hours): 100.00

NASA SOC
(Dollars): 12400.00

NASA NOC
(Hours):

NASA NOC
(Dollars):

Other Costs
(Hours):

Other Costs
(Dollars):

Total Costs in Hours and Dollars are automatically calculated as the sum of the individual costs above. Center IR teams or managers should enter the Center costs, the NASA SOC Manager should enter the SOC Costs and the NOC Manager should enter the NOC costs, if any, in order to arrive at the Total Cost.

Total Cost
(Hours): 389

Total Cost
(Dollars): 41300

Description of
Costs:

System Down
Time (Days):

System Down
Time (Hours):

Timeline

Date Record
Opened (UTC): 1/29/2016 4:32 PM

Date Record
Confirmed
(UTC): 7/16/2016 4:32 AM

Date Record
Contained
(UTC): 7/15/2016 5:37 PM

Date Record
Resolved (UTC): 7/15/2016 5:37 PM

Date Record
Closed (UTC): 7/16/2016 6:07 AM

Time in Open: 168.50

Time in
Confirmed:

Time to
Confirm: 168.00

Time in
Contained: 0.52

Time to Contain: 168.05

SENSITIVE BUT UNCLASSIFIED

Time in Resolved: 0.520833

Time to Resolve: 168.05

Time in Closed: 976.95

Time to Close: 168.57

Number of Days to Resolve: 168.045

Journal Entries

Entry	Entry Date	IMS User
Received AFRCs hours 196 hrs = 19,600. Attached the spreadsheet provided.	9/28/2016 12:53 AM	(b) (6)
Updated ticket to reflect Center's hours listed in journal. Break out as follows: GSFC 23 hrs = \$2300. GRC 70 hrs = \$7000. Spoke to (b) (6) of AFRC and he is getting me his Center's hours here shortly. Once I receive I will update the ticket.	9/27/2016 9:38 PM	(b) (6)
Updated SOC TVA hours 50 = \$5000. SOC Management hours 10 = \$1000	9/27/2016 9:30 PM	(b) (6)
Updated SOC hours, 24 hrs for T3 = \$4800. 16 hours for T2 = \$1600.	9/27/2016 8:55 PM	(b) (6)
Total hours spent so far between both investigations is 18 hours.	2/9/2016 5:47 PM	(b) (6)
Attached the Close Caption TV IP address list. This list contains ~308 cameras with type and models used by (b) (6)	2/4/2016 8:46 PM	(b) (6)
GRC IRT is recording 70 hours of time spent on the 649963 Data Breach Incident. This includes an Estimate of all Center hours (Center Director, A-Staff, CIO, DCIO, CISO, IRM, IRT, CI, Export Control).	2/4/2016 4:47 PM	(b) (6)
GRC Export Control Administrator determined that all UAV work at GRC was not related to this project. GRC IRT performed proxy (Web Content Filter) Log Analysis, Firewall Log Analysis and other data analysis. GRC IRM, CISO and IRT communicated incident with GRC Leadership, Export Control and Counterintelligence. We will update this journal entry if any additional hours are recorded or additional work is performed.		
(From IVV security admins)	2/3/2016 3:55 PM	(b) (6)
(b) (6) ,		
Here is what we know:		
-There has been no user named (b) (6), associated with IV&V since at least 2011. It could be further but we don't have logs/paperwork before that -There is no username in ID.nasa.gov ever associated with IV&V. This goes back to about 2009 -There is no record of (b) (2), (b) (7) on the IV&V tools network. We have logs dated back		

SENSITIVE BUT UNCLASSIFIED

through 2012 that verify no such IP was ever used
 -There are never unix/linux machines on the
 (b) (2), network. This is a windows only network
 -There is no record of our Intrusion prevention
 system have any record of any of these rooted
 events. It would notify us if such an event
 occurred and block if from passing any traffic.

I suspect this is a spoofed IP that IPAM just
 picked up but it looks to be external.

Call me if you have any questions but I don't
 believe there is any association with IV&V with
 this event.

Thanks

(b)

Adding host (b) (2), (b) (7)(E) after 2/3/2016 3:39 PM
 identifying the hostname match from the reporting. Alerted GSFC of the
 new development.

(b) (6)

New pastebin likely listing download sites for OpNasa hack dump data. 2/3/2016 3:27 PM

(b) (6)

<http://pastebin.com/gxwjfzCa>

magnet:?xt=urn:btih:8E0C7D985504BF6829644D650F1102C49AC35FB4
 &dn=250GB_OpNasaDrones_Logs.zip&tr=udp%3a%2f%2ftracker.openbit
 torrent.com%3a80%2fannounce&tr=udp%3a%2f%2ftracker.publicbt.co
 m%3a80%2fannounce&tr=udp%3a%2f%2ftracker.ccc.de%3a80%2fannou
 nce&tr=udp%3a%2f%2ftracker.openbittorrent.com%3a80%2fannounce&
 tr=udp%3a%2f%2ftracker.publicbt.com%3a80%2fannounce&tr=udp%3a
 %2f%2ftrackr.sytes.net%3a80&tr=udp%3a%2f%2fopen.demonii.com%3a
 1337&tr=udp%3a%2f%2ftracker.coppersurfer.tk%3a6969&tr=udp%3a%2
 f%2ftracker.leechers-
 paradise.org%3a6969&tr=udp%3a%2f%2ftracker.openbittorrent.com%3
 a80&tr=http%3a%2f%2ftracker.dutchtracking.com%2fannounce&tr=http
 %3a%2f%2ftracker.dutchtracking.nl%2fannounce&tr=http%3a%2f%2fa.tr
 acker.thepiratebay.org%2fannounce&tr=http%3a%2f%2fbestrepack.net
 %2fbt%2fannounce.php%3fuk%3dCqFMANJfqG&tr=http%3a%2f%2fbt.g
 oldenshara.net%2fbt%2fannounce.php%3fuk%3dMdPQ2kmV1g%26&tr=
 http%3a%2f%2feztv.tracker.thepiratebay.org%2fannounce&tr=http%3a
 %2f%2fopen.tracker.thepiratebay.org%2fannounce&tr=http%3a%2f%2fp
 ow7.com%2fannounce&tr=http%3a%2f%2fpow7.com%3a80%2fannounc

SENSITIVE BUT UNCLASSIFIED

e&tr=http%3a%2f%2ft1.pow7.com%2fannounce&tr=http%3a%2f%2ft2.p
ow7.com%2fannounce&tr=http%3a%2f%2ftpb.tracker.thepiratebay.org
%2fannounce&tr=http%3a%2f%2ftracker.pow7.com%2fannounce&tr=ht
tp%3a%2f%2ftracker.tfile.me%2fannounce&tr=http%3a%2f%2ftracker.th
epiratebay.org%2fannounce&tr=http%3a%2f%2ftracker.thepiratebay.org
%2fannounce.php&tr=http%3a%2f%2ftracker2.torrentino.com%2fannou
nce%3fpaskey%3d00000000000000000000000000000000&tr=http%3a
%2f%2ftv.tracker.thepiratebay.org%2fannounce&tr=udp%3a%2f%2f11.r
arbg.com%3a80%2fannounce&tr=udp%3a%2f%2f9.rarbg.com%3a2710%
2fannounce&tr=udp%3a%2f%2f9.rarbg.me%3a2710%2fannounce&tr=ud
p%3a%2f%2fteztv.tracker.thepiratebay.org%3a80%2fannounce&tr=udp%
3a%2f%2fopen.demonii.com%3a1337%2fannounce&tr=udp%3a%2f%2ft
racker.coppersurfer.tk%3a6969%2fannounce&tr=udp%3a%2f%2ftracker.
openbittorrent.com%3a80&tr=udp%3a%2f%2ftracker.openbittorrent.co
m%3a80%2fannounce&tr=udp%3a%2f%2ftracker.seedceo.com%3a2710
%2fannounce&tr=udp%3a%2f%2ftracker.tntvillage

Changed Center Affected from "GSFC" to "Other" to reflect multi-Center
area of effect of investigation. 2/3/2016 5:47 AM

(b) (6)

***** *BEGIN ENCRYPTED or SIGNED PART*

2/2/2016 6:34 PM

(b) (6)

NASA SOC,

Is there an update available on this RFI? The
Infowars.com article now includes the following
"NASA Update":

"UPDATE - NASA's Response to Hack Report:

"Control of our Global Hawk aircraft was not
compromised. NASA has no evidence to indicate the
alleged hacked data are anything other than
already publicly available data. NASA takes

SENSITIVE BUT UNCLASSIFIED

cybersecurity very seriously and will continue to fully investigate all of these allegations."

Is this a legitimate update from NASA? We greatly appreciate your assistance.

Respectfully,

US-CERT Security Operations Center (US-CERT SOC)
National Cybersecurity & Communications
Integration Center (NCCIC) Department of Homeland
Security

(b) (7)(C) / 888-282-0870

SOC@us-cert.gov

[www\[dot\]us-cert.gov](http://www[dot]us-cert.gov)

Twitter: @USCERT_gov

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

-----Original Message-----

From: NASA SOC

(b) (6)

Sent: Monday, February 01, 2016 6:20 PM

To: SOC; National Aeronautics and Space
Administration

Subject: Re: US-CERT Incident number
INC000010050196

* PGP Decrypted Message

Hi,

SWI-20160201-650198 has been created for this incident.

Thanks,

(b)

On 02/01/2016 10:19 AM, soc@us-cert.gov wrote:

***** *BEGIN ENCRYPTED or SIGNED PART*

NASA SOC,

US-CERT received a report of the following
Infowars.com article "Hackers Allegedly Hijack
Drone After Massive Breach at NASA:
[hxxp\[dot\]www\[dot\]infowars.com/hackers-allegedly-hijack-drone-after-massive-breach-at-nasa/](http://hxxp[dot]www[dot]infowars.com/hackers-allegedly-hijack-drone-after-massive-breach-at-nasa/).

Are you aware of the report and able to confirm its validity? Thanks for your assistance.

Respectfully,

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

Email from ticket 650075 in reference from data dump which is in
pastebin.txt :

2/2/2016 4:34 PM

(b) (6)

SOC;

Please open an IMS ticket; attached is information reported by the FBI identified through open source below is a summary, the information date is believed to be sometime in Jan 2016. The open source information seem to claim that a compromise happened on (b) (7)(E) and (b) (7)(E) (possibly used or administrated by (b) (6), (b) , ARC).

Subject: Potential NASA/AnonSec intrusion

Chapters 1-4 of the document largely appear to be a mix of open source information, exaggerations, and old data (see the end of this message for more details)

Chapters 5 and 6 may correspond to a recent but remediated intrusion of NASA systems. It appears AnonSec may have gained (and then lost) access to at least two unclassified/internet-connected systems associated with (b) (6), (b) (b) (7)(E), (b) (7)(C) an (b) (6), (b) (7)(C) at NASA's (b) (b) (6), (b) (7)(C) utilizes (7) Global Hawk drones associated with the Dryden Flight Research Center.

Specifically, AnonSec claims to have accessed at least two Linux systems associated with (b) (6), and three Western Digital NAS drives containing (b) (6), (b) (7)(C)

. They also claim (b) (7) (E), (b) (7)(C) I find that last claim fairly dubious, but not impossible.

It's unclear when this intrusion supposedly occurred. However, searching for the hashtag OpNasaDrones on twitter revealed posts by Anon members appearing to refer to this intrusion

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

dating back to January 2015 or even late 2014. In terms of the end date for the intrusion, AnonSec claims NASA discovered the attack and completely locked them out. Assuming the zine was recently published, this remediation may have also occurred recently. In fact, a tweet one hour ago by OpNasaDrones states "T-Minus 24hrs until #OpNasaDrones leaks & zine released..."

Along with the zine, (b) (7)(E)

I believe the FBI has not yet retrieved the full dataset yet.

Analysis of Chapters 1-4:

(b) (7)(E)

- Lines 351-359 (b) (7)(E)

in Chapters 5,6

- From there, (b) (7)(E)

:

- (b) (7)(E)

- (b) (7)(E)

So that's (b) (7)(E)

- Lines 509-510 are interesting. (b)

(7)

(E)

SENSITIVE BUT UNCLASSIFIED

Additional information has been provided in the following tickets and have been merged into this ticket.

2/2/2016 4:08 PM

(b) (6)

SOC-20160130-650046

SOC-20160131-650075

Calldown requested by SOC T2 on 2/1/16 at 3:17PM, T1 reached (b) (6) at 2/1/16 8:05PM.

2/2/2016 4:11 AM

(b) (6)

Here are the notes I took after thoroughly reviewing the "zine" they posted. All these things are "allegedly" since we can't find any evidence to substantiate ANY of the claims. Still need to try to find evidence of when this alleged flight was that they tried to crash the drone into the ocean. So far, I don't see anything here that you couldn't either get from a public source, or simply fabricate. The portions where they show themselves issuing commands seem especially elaborate to fabricate, but it's certainly still possible they made all this up.

2/1/2016 9:47 PM

(b) (6)

Compromised machines:

(b) (6)

(b) (6)

Reported NAS names (2TB WD My Book World Edition):

DRONE_BACKUPS

DRONE_BACKUPS2

DRONE_BACKUPS3

192.168.3.17 (potentially an IP for one of the NAS devices)

192.168.3.18 (potentially an IP for one of the NAS devices)

192.168.3.19 (potentially an IP for one of the NAS devices)

Picture of (b) (6) lifted from here:

(b) (7)(E)

PDF of Armstrong Flight Research Center Axis IP camera upgrade available here:

(b) (7)(E)

They link it as

(b) (7)(E)

JSC:

Reportedly compromised a bunch of axis IP cameras using a RAT malware tool on NASA employee (b) (6) computer.

https://(b) (6)

https://(b) (6)

They posted a screenshot of a "pilot proficiency test" which looks like it came from this public page:

https://espo.nasa.gov/flight_reports/Global_Hawk_872_04_09_15

"Logic Bomb" files (we can probably get hashes of these for sweeps if needed):

nyan.sh - From <https://github.com/klange/nyancat>

guardian.pl

Failsafe.sh

SENSITIVE BUT UNCLASSIFIED

C2.2.1.01.conf

attacker handles:

d3f4ult

Shimo7even

martybugs

Bashtien

Sh1n0d4

c2 domains noted:

(b) (7)(E)

co.uk - used to host scripts

- used to host bad firmware

used to (b) (7)(E)

email address used in

notification of logic bomb execution

SENSITIVE BUT UNCLASSIFIED

Below is a draft update of the originally approved statement for the press that includes a mention of the drone, without committing to anything.

2/1/2016 8:02 PM

(b) (6)

It appears there was no breach of any mission critical systems or data. NASA takes cybersecurity very seriously, as well as the allegation regarding the potential illegal use of one of our scientific research unmanned aircraft systems. NASA strives to make our scientific data publically available, including large data sets, which seems to be how the information in question was retrieved. Our Open Data websites offer easier access and use of NASA data through tools and shared experiences using over 30,000 datasets, 192 shared code, 36 API's, and more:

- [Open.NASA.gov](https://open.nasa.gov)
- [Data.NASA.gov](https://data.nasa.gov)
- [API.NASA.gov](https://api.nasa.gov)
- [Code.NASA.gov](https://code.nasa.gov)
- [GitHub.com/NASA](https://github.com/NASA)

2/1/2016 3:36 PM

(b) (6)

The GSFC Incident Response team has reviewed the sample data which was attached to this incident.

Investigation Results

1. One of the websites in the sample data is a NASA website, the other is a University of North Dakota website.
2. Investigation determined that the NASA website (see URL below) is an ARC device.
3. No GSFC hosts were included in the sample data.
4. Given this result – there are no further actions for GSFC Incident Response at this time.

Notes

The data in the sample itself appear to indeed be telemetry data (but it appears to very likely be public data).

The owner of the site would have to

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

confirm whether or not this data was indeed publicly available.

The following Google search term below revealed that this data is available via an Excel spreadsheet published on the website in question:

<https://www.google.com/search?q=%22ACCESS+II+2014+-+Alternative-Fuel+Effects+on+Contrails+and+Cruise+EmiSSions+2014%22&client=safari&rls=en&filter=0&biw=1467&bih=991>

Websites referenced in the sample data

https://airbornescience.nasa.gov/sites/default/files/DC8_Experimenter_Handbook_Jan2011v2.pdf

NASA Airborne Science Program

<http://www.nserc.und.edu/about/contact.html>

The National Suborbital Education and Research Center (NSERC) is the product of a cooperative agreement between NASA and the University of North Dakota.

IMS Ticket Number: SOC-20160129-649963

(b) (6)

SENSITIVE BUT UNCLASSIFIED

Uploaded a copy of the pastebin dump.	2/1/2016 10:00 AM	(b) (6)
(b) (6)	1/29/2016 10:39 PM	(b) (6)
Notified Tier-1 to include his contact information for this ticket:		
(b) (6)		
(b) (6)		
(b) (6)		
Call down completed with LARC and AFRC.	1/29/2016 9:21 PM	(b) (6)
I just talked with (b) (6) the Head of the Langley Atmospheric Data Center and he confirmed any data on science.larc.nasa.gov is configured to be public and as such is approved for public release and dissemination.	1/29/2016 9:19 PM	(b) (6)
GRC IRT reached out to GRC Export Control Representative. He has reached out to an individual at GRC that works on the project.	1/29/2016 8:55 PM	(b) (6)

Here is the website for Nserc: http://www.nserc.und.edu/		
I contacted a researcher here at GRC who I believe has been involved with the University of North Dakota. I will let you know what I find out.		
Steven		

(b) (6)		
(b) (6) ator		
Including search engine results. Please review. These datasets appear to be relative to this attachment:	1/29/2016 8:42 PM	(b) (6)
https://www.google.com/search?q=%22ACCESS+II+2014+-+Alternative-Fuel+Effects+on+Contrails+and+Cruise+EmiSSions+2014%22&btnG=Search		
http://science.larc.nasa.gov/large/data/ACCESS-2/data/		
Call down conducted with GSFC, GRC.	1/29/2016 8:24 PM	(b) (6)

SENSITIVE BUT UNCLASSIFIED**Attachment(s)**

Name	Size	Type	Upload Date	Downloads
_Potential_NASA_AnonSec_intrusion.eml	478049	.eml	2/2/2016 4:30 PM	6
CCTV Spreadsheet 020316.xlsx	19920	.xlsx	2/4/2016 8:45 PM	5
Copy of AFRC-Cost_Tracking_AnonSec (2).xlsx	9096	.xlsx	9/28/2016 12:56 AM	4
Large data breach at NASA.eml	7160400	.eml	1/29/2016 4:31 PM	30
pastebindump.txt	305133	.txt	2/1/2016 10:01 AM	27
Reporting_chatter_of_data_dump_tomorrow.eml	13124	.eml	2/2/2016 4:43 PM	6

History Log[View History Log](#)